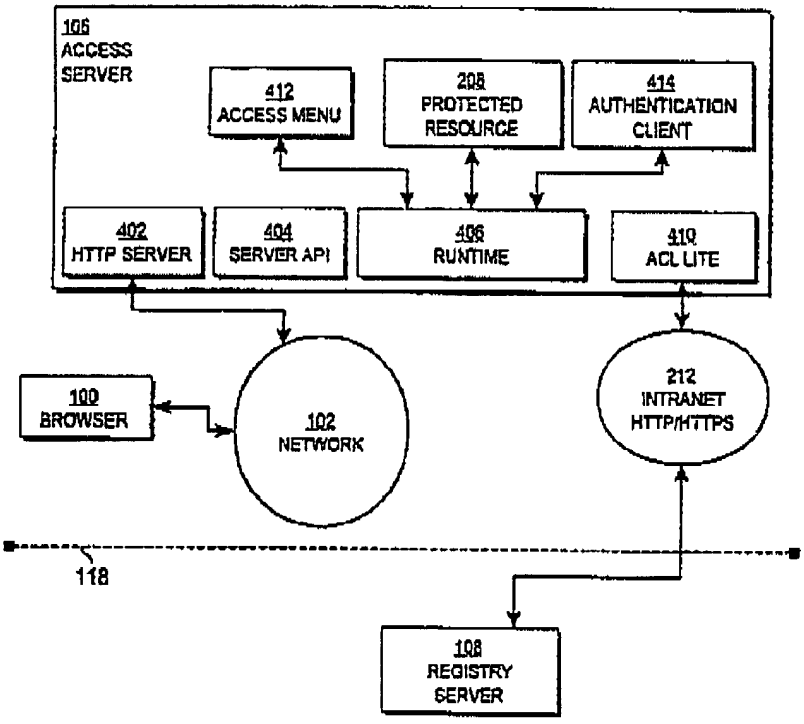
REMARKS

Claims 1-59 are pending and stand rejected. Claims 1, 5, 6, 14, 21, 25, 26, 32, 38, 44, 49, and 54 have been amended.

CLAIM REJECTIONS – 35 USC § 103: The Examiner rejected Claims 1-12, 14-19, 21-30, 32-42, 44-51, 54-56, and 58-59 as being unpatentable over USPN 6,453,353 issued to Win in view of US Pub. 2003/0061275 to Brown.

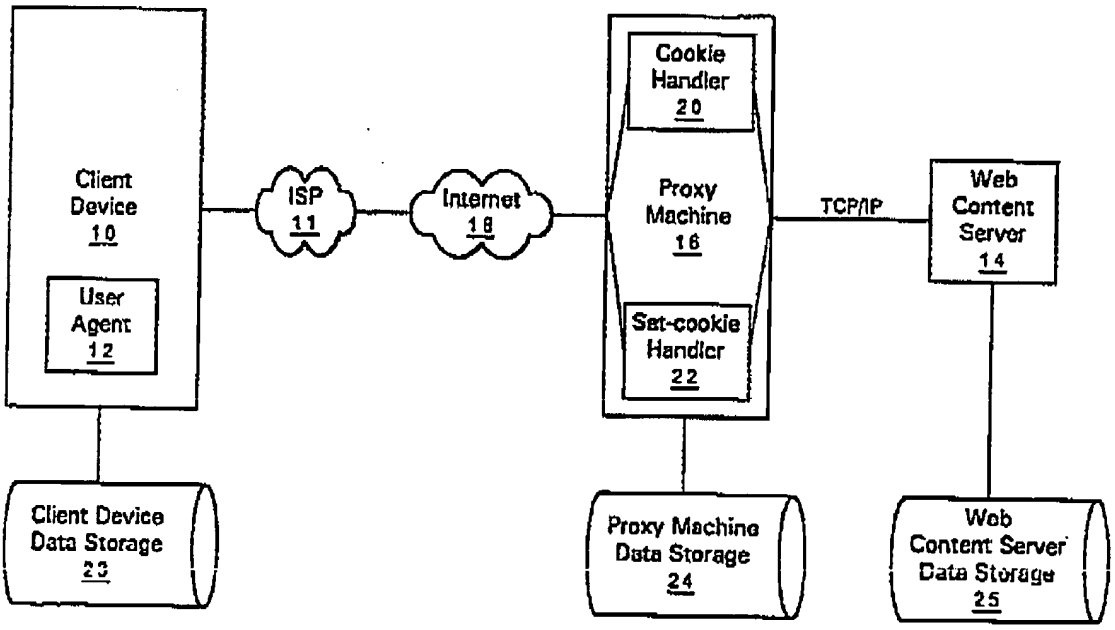
Win describes a system in which a user can gain access to authorized web based resources based on the user's role in an organization. *See, e.g.*, Win Abstract. Win's system includes an Access server (106) and a registry server (108) that help regulate to a protected resource (208). *See* Win, Fig. 4 (reproduced below).



The following summary is taken from Win, col. 4, line 33 through col. 6, line 65. To access a protected resource (208) via browser (100), the user is first presented with a login page. Win's authentication client (414) verifies credentials entered through the

page and reads the user's "roles" from the registry server (108). Authentication client (414) then encrypts and sends this data as a cookie to browser (100). Once the user is authenticated, access menu (412) returns a menu personalized according to the user's roles. That menu provides access to one or more protected resources. Browser (100) is required to supply the cookie to enable the user to access any of those resources.

Brown simply describes a proxy machine (16) capable of stripping "set cookie" commands being returned in message headers to a client device (10) from a web content server (14). The proxy machine (16) stores the cookie in a storage (24) so that the client device (10) does not have to. The proxy machine (16) also functions to add cookies to message headers being sent from the client device (10) to the web content server (14).



Claim 1 is directed to a method for providing a first network resource operating on a first network device access to a second network resource operating on a second network device. Claim 1 recites the following acts:

1. from a third network device, locating a profile using profile data obtained from a client device, the profile containing data for identifying and for accessing the second network resource;
2. from the third network device, supplying the profile to the second network resource;
3. at the third network device, receiving temporary credentials for accessing the second network resource and generated according to the profile, the temporary credentials being provided from the second network resource; and
4. from the third network device, providing the first network resource with the temporary credentials so that the first network resource can provide the second network resource with the temporary credentials to access and interact with the second network resource on behalf of the client device.

The Examiner asserts that Win teaches all of Claim 1 except providing the first network resource with the temporary credentials so that the first network resource can provide the second network resource with the temporary credentials to access and interact with the second network resource on behalf of the client device. Addressing this deficiency, the Examiner relies on Brown.

Win and Brown do not teach or suggest, at the third network device, receiving temporary credentials for accessing the second network resource and generated according to the profile, the temporary credentials being provided from the second network resource. With respect to this third element of Claim 1, the Examiner, relying only on Win, cites Win, col. 6, lines 48-54 and col. 10, line 51 through col. 11, line 9. The Examiner asserts "Win's access server generates a temporary cookie that is transmitted to the user, and the cookie provides the information that enables a user- to access his resources based on his profile (role)."

Initially, it is important to note that (1) the Examiner equated Win's access server (108) with the first network resource/device recited in Claim 1 (see page 3 of the of the Office Action mailed 12/28/2005), and (2) the Examiner equated Win's registry server

with the third network device recited in Claim 1 (see page 5 of the Office Action Mailed 12/28/2005).

The third element of Claim 1, listed above, explicitly recites – at the third network device, receiving temporary credentials for accessing the second network resource and generated according to the profile where the temporary credentials are received from the second network resource which operates on a second network device. To restate, the temporary credentials are received at the third network device and are provided from the second network device.

As noted above, the Examiner equates Win's registry server with the third network device and Win's access server with the second network device/resource recited in Claim 1. However, Win's access server (*compare wit the first network recource/device*) does not provide Win's registry server (*compare with the third network device*) with temporary credentials. Restated, temporary credentials provided by Win's access server are never received at Win's registry server. Instead, as the Examiner admits, Win's access server generates a cookie that is transmitted to the user. That cookie is not received at Win's registry service and therefore is not provided to Win's registry server from Win's access server.

Win and Brown do not teach or suggest, from the third network device, providing the first network resource with the temporary credentials so that the first network resource can provide the second network resource with the temporary credentials to access and interact with the second network resource on behalf of the client device. With respect to this fourth element of Claim 1, the Examiner, relying only on Brown asserts "Brown discloses providing the first network resource with the temporary credentials so that the first network resource can provide the second network resource with the temporary credentials to access the second network resource on behalf of the client device. In support, the Examiner cites Brown, paragraphs [0012], [0026], and [0027] and asserts Brown's "the proxy server is supplied with the temporary credentials from the web server.

It is important to note that the Examiner has left out and not addressed a portion of this fourth element. The Examiner ignores that that the fourth element explicitly recites that the temporary credentials are provide to the first network resource **from the third network device**.

The Examiner's rejection equates Brown 's proxy machine (16) with the first network resource/device recited in Claim 1. The Examiner's rejection also equates Brown's web content server (14) with the second network resource/device recited in Claim 1. Brown's web content server (16) provides Brown's proxy machine (16) with a persistent cookie. Brown's proxy machine (16) provides that cookie back to Brown's web content server (14) upon intercepting a request from Brown's client device (10) directed to Brown 's web content server (I4).

Claim 1 explicitly recites that temporary credentials are provided from the third network device to the first network resource while Brown's cookie is provided from Brown's web content server (the second network resource/device) to Brown's proxy machine (the first network resource/device). Brown only teaches communication of a cookie between two devices, Brown's proxy machine and Browns web content server. Because Brown's cookie is not provided to Brown's proxy machine from a network device other than Brown's web content server – Brown does not teach or suggest a method in which temporary credentials are provide to the first network resource **from the third network device** so that the first network resource can access and interact with a second network resource on behalf of the client device in the manner recited by Claim 1.

For at least these reasons, Claim 1 is patentable over Win and Brown as are Claims 2-5 due at least in part to their dependence from Claim 1.

Claim 6 is directed to method for enabling an application server to access a data service, the application server operating on a first network device and the data service operating on a second network device, and recites the following acts:

1. the application server instructing a client device to provide profile data to an identification service operating on a third network device, the identification service having access to one or more profiles used to access one or more data services including the data service operating on the second network device, the profile data identifying a particular profile;
2. the identification service locating the particular profile using the profile data received from the client device, the profile containing data for identifying and for accessing the data service;
3. the identification service providing the profile to the data service;
4. the data service generating temporary credentials for accessing the data service identified by the particular profile and providing the temporary credentials to the identification service; and
5. the application server obtaining the temporary credentials from the identification service and providing the data service with the temporary credentials to access and interact with the data service on behalf of the client device.

The Examiner asserts that Win teaches all of Claim 6 except the application server obtaining the temporary credentials and providing the data service with the temporary credentials to access and interact with the data service on behalf of the client device. Addressing this deficiency, the Examiner relies on Brown.

Win and Brown do not teach or suggest the data service generating temporary credentials for accessing the data service identified by the particular profile and providing the temporary credentials to the identification service. With respect to this fourth element, the Examiner cited Win, col. 6, lines 48-54. With respect to Claim 1, it was clarified above that Win (and Brown) fail to teach or suggest, at a third network device, receiving temporary credentials for accessing a second network resource that operates on a second network device where the temporary credentials are provided from the second network resource. Similarly and for the same reasons specified above, Win (an Brown) fail to teach or suggest a method in which a data service (the second network resource/device) generates temporary credentials for accessing the

data service identified by the particular profile and provides the temporary credentials to the identification service (the third network device).

In comparison, Win's access server (*compare to the recited data service*) does not provide Win's registry server (*compare to the recited identification service*) with temporary credentials. Restated, temporary credentials are never provided by Win's access server and then received at Win's registry server. Instead, as the Examiner admits, Win's access server generates a cookie that is transmitted to the user. That cookie is not received at Win's registry service and therefore is not provided to Win's registry server from Win's access server.

Win and Brown do not teach or suggest the application server obtaining the temporary credentials from the identification service and providing the data service with the temporary credentials to access and interact with the data service on behalf of the client device. With respect to this fifth element of Claim 6, the Examiner cited Brown, paragraphs [0019], [0020], and [0022]. It is noted that, with respect to Claim 1, it was clarified above that Brown (and Win) fail to teach or suggest a method that includes receiving, at a third network device, temporary credentials for accessing a second network resource and generated according to the profile where the temporary credentials are provided from that second network resource. Similarly and for the same reasons specified above, Brown (and Win) fail to teach or suggest a method in which an application server obtains the temporary credentials from an identification service and provides a data service with the temporary credentials to access and interact with the data service on behalf of a client device.

Brown's proxy machine (16) receives a cookie from the same device, web content server (14), it later provides that cookie to. In comparison, Claim 6 recites that temporary credentials are obtained by an application server from an identification service and that the application server provides those temporary credentials to a data service. The data service recited in Claim 6 is different than the application server recited in Claim 6.

For at least these reasons, Claim 6 is patentable over Win and Brown, as are Claims 7-13 which depend from Claim 6.

Claim 14 is directed to a method for enabling an application server to access a data service, the application server operating on a first network device and the data service operating on a second network device, and recites the following acts:

1. the application server receiving, from a client device, a request to direct an application;
2. the application server instructing the client device to provide profile data to an identification service operating on a third network device, the identification service having access to one or more profiles for identifying and accessing one or more data services, the profile data identifying a particular profile;
3. the identification service providing the data service with the particular profile identified by the profile data, the profile containing data for identifying and accessing the data service;
4. the data service using the profile to generate temporary credentials for accessing the data service and providing the temporary credentials to the identification service; and
5. the application server obtaining the temporary credentials from the identification service and providing the data service with the temporary credentials to access and interact with the data service on behalf of the client device.

In the spirit of Claim 6, Claim 14 recites the data service using a profile to generate temporary credentials for accessing the data service and providing the temporary credentials to the identification service and the application server obtaining the temporary credentials from the identification service and providing the data service with the temporary credentials to access and interact with the data service on behalf of the client device. As with Claim 6, this is neither taught nor suggested by the combined teachings of Win and Brown.

For at least this reason Claim 14 is patentable over Win and Brown as are Claims 15-20 which depend from Claim 14.

Claim 21 is directed to a computer readable medium having instructions for implementing the method steps similar to those of Claim 1. For the same reasons Claim 1 is patentable, so are Claim 21 and Claims 22-25 which depend from claim 21.

Claim 26 is directed to a computer readable medium having instructions for implementing the method steps similar to those of Claim 14. For the same reasons Claim 14 is patentable, so are Claim 26 and Claims 27-31 which depend from Claim 26.

Claim 32 is directed to a computer readable medium having instructions for:

1. from a third network device, generating an interface having user accessible controls for creating a profile for accessing a data service operating on a second network device;
2. from the third network device, creating a profile according to selections made through the interface the profile containing data for identifying and accessing the data service; and
3. from the third network device:
    a. providing a client device with profile data identifying a created profile;
    b. upon receiving the profile data from the client device, retrieving a profile identified by the profile data;
    c. generating temporary credentials for accessing the data service identified by the retrieved profile; and
    d. providing an application server operating on a first network device with the temporary credentials for accessing and interacting with the data service on behalf of the client device.

In the spirit of Claim 1, Claim 32 recites providing, from a third network device, an application server (operating on a first network device) with temporary credentials for accessing and interacting with a data service (operating on a second network device)

on behalf of a client device. Those temporary credentials are generated according to a profile retrieved using profile data. As with Claim 1, this is neither taught nor suggested by the combined teachings of Win and Brown.

For at least these reasons Claim 32 is patentable over Win and Brown as are Claims 33-37 which depend from Claim 32.

Claim 38 is directed to a computer readable medium having instructions for:

1. generating, at a third network device, a profile interface having user accessible controls for creating a profile for locating and accessing a data service operating on a second network device;
2. from the third network device, creating a profile according to selections made through the profile interface, the profile containing data for identifying and accessing the data service;
3. from the third network device, providing a client device with profile data identifying a created profile;
4. receiving, at a first network device, a request to access an application;
5. from the first network device, instructing a client device to send profile data;
6. receiving the profile data at the third network device;
7. from the third network device, retrieving a profile identified by the profile data;
8. generating, at the second network device, temporary credentials for accessing a data service identified by the retrieved profile and providing the temporary credentials to the third network device; and
9. at the first network device, obtaining the temporary credentials from the third network device and providing the data service with the temporary credentials to access and interact with the data service on behalf of the client device.

In the spirit of Claim 6, Claim 38 recites providing, from a first network device, a data service with the temporary credentials to access and interact with the data service (operating on a second network device) on behalf of a client device. Those temporary credentials are generated at the second network device according to a profile retrieved

using profile data and provided to a third network device. The temporary credentials are obtained at the first network device and then provided to the data service to be used to access and interact with the data service on behalf of the client device. As with Claim 6, this is neither taught nor suggested by the combined teachings of Win and Brown.

For at least these reasons Claim 38 is patentable over Win and Brown as are Claims 39-43 which depend from Claim 38.

Claim 44 is directed to a system for providing a first network resource operating on a first network device with access to a second network resource operating on a second network device and recites the following elements:

1. an identification service operating on a third network device, the identification service in network communication with a credential module,
2. the credential module operating on the second network device and operable to use a profile acquired by the identification service to generate temporary credentials for accessing the second network resource;
3. the identification service being operable to receive profile data from a client device, to acquire a profile identified by the profile data;
4. the credential module and the identification service, together being operable to provide the first network resource with the temporary credentials enabling the first network resource to provide the second network resource with the temporary credentials to access and interact with the second network resource on behalf of the client device.

Similar to the previous Claims, Claim 44 recites a credential module (operating on a second network device) and an identification service (operating on a third network device) that together can provide a first network resource (operating on a first network device) with the temporary credentials enabling the first network resource to provide a second network resource (operating on the second network device) with the temporary credentials to access and interact with the second network resource on behalf of a

client. This is neither taught nor suggested by the combined teachings of Win and Brown.

For at least this reason Claim 44 is patentable over Win and Brown as are Claims 45-48 which depend from Claim 44.

Claim 49 is directed to a system for accessing a data service operating on a second network device and recites the following elements:

1. an identification service, operating on a third network device, operable to receive profile data from a client device identifying a particular profile and to provide that profile, the profile to contain electronic data used to identify the data service;
2. a credential module, operating on the second network device, operable to obtain the profile from the identification service, generate temporary credentials, and map those credentials to the data service identified by the profile; and
3. an application server, operating on a first network device, operable to serve an interface containing instructions to send profile data to the identification service, to obtain the temporary credentials, and to provide the data service with the temporary credentials to access and interact with the data service on behalf of the client device.

Win and Brown do not teach or suggest an identification service, a credential module, and an application server where each of those elements operates on a different network device in the manner recited. For at least this reason Claim 49 is patentable over Win and Brawn as are Claims 50-53 which depend from Claim 49.

Claim 54 is directed to a system for accessing a data service operating on a second network device and recites the following elements:

1. an identification service operating on a third network device and operable to generate a profile interface having user accessible controls for creating a profile

containing electronic data used to identify the data service, to create a profile using selections made through the profile interface, to issue instructions to store profile data used to access the created profile, to receive, from a client device, profile data identifying a particular profile, and to provide that profile;

2. a credential module operable to obtain the profile from the identification service, generate temporary credentials, and map those credentials to the data service identified by the profile; and
3. an application server operating on a first network device and operable to serve an application interface that includes instructions to send profile data to the identification service, to obtain the temporary credentials, and to provide the data service with the temporary credentials to access and interact with the data service on behalf of the client device.

Win and Brown do not teach or suggest an identification service, a credential module, and an application server where each operates on a different network device in the manner recited. For at least this reason Claim 54 is patentable over Win and Brown as are Claims 55-58 which depend from Claim 54.

Claim 59 is directed to a system for accessing data and recites the following elements:

1. a means for generating a profile interface having user accessible controls for creating a profile containing electronic data used to identify a particular data service operating on a second network device;
2. a means for creating a profile using selections made through the profile interface;
3. a means for issuing instructions to store profile data used to access the created profile;
4. a means for receiving, from a client device, profile data identifying a particular profile;
5. a means for providing the particular profile;

6. a means for generating temporary credentials;
7. a means for mapping the temporary credentials to the data service identified by the provided profile;
8. a means for serving an application interface that includes instructions to send profile data to an identification service operating on a third network device;
9. a means for providing, from a first network device, the data service with the temporary credentials to access and interact with the data service on behalf of the client device; and
10. a means for invalidating the temporary credentials

Win and Brown fail to teach or suggest a system that utilizes three different network devices and a client device in the manner recited by Claim 59. For at least this reason Claim 59 is patentable over Win and Brown.

CLAIM REJECTIONS – 35 USC § 103: The Examiner rejected Claims 13, 20, 31, 43, 52, 53, and 57 as being unpatentable over Win in view of a publication authored by Curtin.

- Claim 13 depends from Claim 6 and includes all the limitations of that base Claim. For at least the same reasons Claim 6 is patentable, so is Claim 13.
- Claim 20 depends from Claim 14 and includes all the limitations of that base Claim. For at least the same reasons Claim 14 is patentable, so is Claim 20.
- Claim 31 depends from Claim 26 and includes all the limitations of that base Claim. For at least the same reasons Claim 26 is patentable, so is Claim 31.
- Claim 43 depends from Claim 38 and includes all the limitations of that base Claim. For at least the same reasons Claim 38 is patentable, so is Claim 43.
- Claims 52 and 53 depend from Claim 51 and include all the limitations of that base Claim. For at least the same reasons Claim 51 is patentable, so are Claims 52 and 53.

- Claim 57 depends from Claim 54 and includes all the limitations of that base Claim. For at least the same reasons Claim 54 is patentable, so is Claim 57.

CONCLUSION: The foregoing is believed to be a complete response to the outstanding Office Action. Claims 1-59 are felt to be in condition for allowance. Consequently, early and favorable action allowing these claims and passing the application to issue is earnestly solicited. The foregoing is believed to be a complete response to the outstanding Office Action.

Respectfully submitted,
Gregory Eugene Perkins

By _____
Jack H. McKinney
Reg. No. 45,685

March 27, 2006